Menjadi Mata-Mata

Pada bab sebelumnya Anda sudah bisa membobol password facebook orang lain yang sebelumnya sudah pernah menggunakan sebuah komputer dan tersimpan dalam komputer tersebut.

Kali ini kita akan meningkat dengan teknik mata-mata, di mana seseorang tidak menyimpan account dan password-nya dalam sebuah komputer. Mungkin saja ada mantan Anda yang pinjam laptop Anda buat membalas status pasangan barunya. Anda bisa memata-matai password-nya.

Cara yang paling mudah untuk mengetahui password dengan metode mata-mata ini adalah dengan melihat karakter yang dipencet oleh orang lain pada keyboard komputer Anda. Gampang kan.

Mungkin banyak yang mengira "itu namanya bukan hacking", tapi itu adalah salah satu strategi yang dikenal sebagai *social engineering*.

Ya, kalau Anda tidak menyukai cara yang satu ini, kita akan menggunakan cara yang sedikit canggih biar gak ketahuan amat ngintipnya.

Unhide Passwords for Firefox

Khusus pula untuk browser Firefox, terdapat sebuah add-ons yang bisa digunakan untuk tujuan yang sama. Saya rasa Anda semua sudah terbiasa mengisi password setiap kali login. Dari sana tampilan password berupa karakter asterisk (*) atau sebuah bulatan hitam.

Bagi Anda yang mau bongkar-bongkar password facebook punya orang, hal ini lebih enak dilakukan di warnet. Kebanyakan orang tidak tahu kalau mereka menyimpan sebuah password ternyata bisa dicuri. Walaupun yang tampil adalah karakter asterisk. Dengan add-ons berikut Anda bisa memunculkannya.

Mungkin Anda bertanya, kenapa bagian ini saya masukkan sebagai teknik mata-mata. Bukankah hal ini sama saja dengan melihat kode asterisk.

Sekilas terlihat sama, dan salah satu fungsinya memang sama. Perbedaan yang utama adalah, teknik ini bisa digunakan untuk memata-matai password. Begini maksudnya, kalau hanya melihat kode asterisk berarti sebelumnya password sudah tertanam dalam sebuah komputer terlebih dahulu. Lain halnya dengan yang satu ini.

Anda tidak perlu menunggu seseorang bersedia menyimpan password di komputer. Anda bisa saja melihat seseorang mengetikkan password (memata-matai). Sebab, sewaktu password diketikkan, yang muncul bukanlah kode asterisk melainkan karakter yang normal yang bisa dibaca. Sehingga Anda bisa mencuri-curi pandang. Apalagi yang *make* pacar Anda yang selalu berusaha menyembunyikan password-nya di depan Anda.

Sekarang, terlebih dahulu, silakan download add-ons-nya pada link berikut:

https://addons.mozilla.org/en-US/firefox/addon/462?application=firefox&numpg=1057&id=462

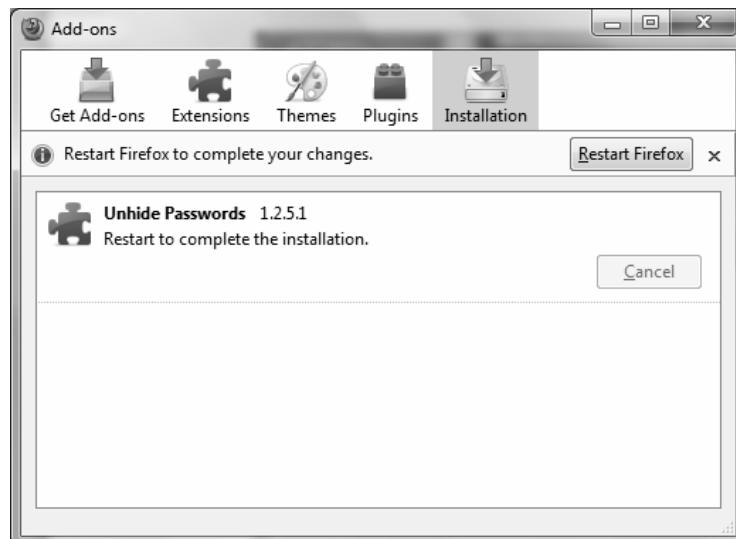
Gambar 4.1 Add-Ons Unhide Passwords

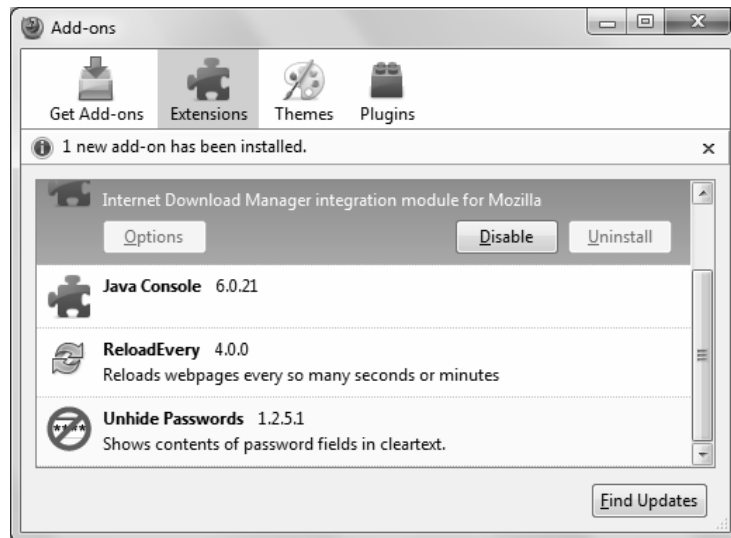
Setelah itu, klik tombol **Add to firefox**, maka akan muncul sebuah kotak dialog untuk instalasi. Klik tombol **Install Now**.

Gambar 4.2 Instalasi Add-Ons

Tunggu proses instalasi dilakukan sampai selesai.

Gambar 4.3 Proses Instalasi

Setelah selesai, Anda diminta untuk me-restart browser Firefox baru bisa menggunakan add-ons tersebut. Klik tombol **Restart Firefox**.

Gambar 4.4 Instalasi selesai

Setelah proses instalasi selesai dilakukan dan halaman Firefox kembali muncul, tutup terlebih dahulu kotak dialog yang menyatakan bahwa proses instalasi add-ons berhasil.

Gambar 4.5 Ads-ons sudah diinstalasi

Untuk menggunakannya, Anda hanya perlu mengarahkan mouse pada tanda asterisk, secara otomatis karakter asterisk akan berubah menjadi huruf atau angka password-nya.

Gambar 4.6 Password menjadi terlihat

Keylogger

Teknik mata-mata lainnya, di sini kita akan menggunakan apa yang disebut dengan keylogger. Keylogger adalah sebuah software yang

digunakan untuk memantau kegiatan keyboard komputer, setiap tombol yang ditekan oleh user maka semua *record* akan disimpan dengan keylogger.

Keylogger merupakan software yang berfungsi untuk memonitoring kegiatan PC dengan me-record/merekam kegiatan keyboard.

Prinsip kerja keylogger adalah, Anda tinggal instal di komputer lalu orang yang menggunakan komputer tersebut akan terekam seluruh kegiatannya termasuk kegiatan memasukkan "password dan username" facebook.

Ada banyak ragam keylogger yang bisa digunakan. Di sini saya menggunakan salah satu keylogger yang bisa Anda gunakan, yaitu Douglas 2.0. Anda bisa men-download-nya di: http://keylogger-douglas.en.malavida.com/download.

Setelah Anda memperoleh file Douglas tersebut, ikuti langkah berikut ini untuk menggunakannya:

1. Lakukan instalasi terlebih dahulu, dengan mengklik file **Install**. Maka akan tampil jendela Welcome, klik saja **Next**.

Gambar 4.7 Halaman depan Keylogger Douglas

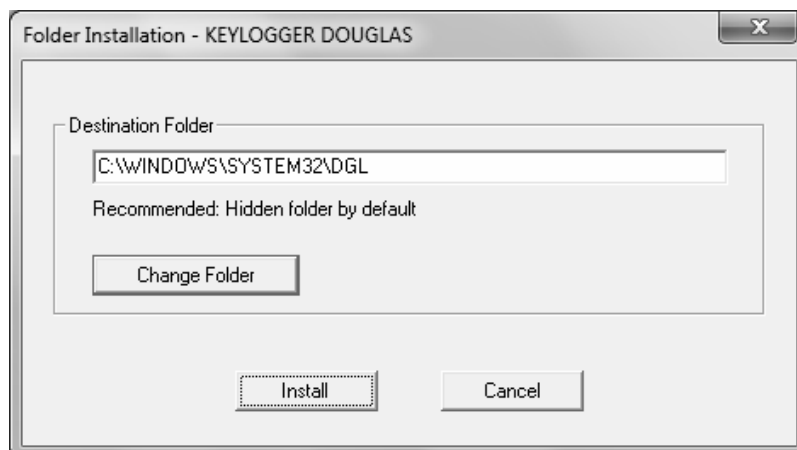
2. Berikan tanda centang pada: *I accept the terms in the License Agreement*, lanjutkan dengan mengklik tombol **Accept**.

Gambar 4.8 Halaman License Agreement

3. Sekarang Anda bisa memilih untuk memasang password pada program tersebut atau tidak supaya tidak sembarang orang bisa melihatnya. Ingat, kalau Anda sampai lupa password maka Anda tidak bisa mengakses informasi yang tersimpan dalam program tersebut, termasuk pula tidak bisa meng-uninstall program itu sendiri.

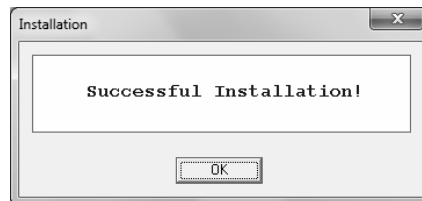
4. Atau, kalau Anda mau aman, serta tidak ingin menggunakan password, berikan tanda centang pada *Don't use password*. Lanjutkan dengan mengklik tombol **OK**.

Gambar 4.9 Memasukkan password

5. Sekarang Anda telah siap untuk melakukan proses instalasi, klik tombol **Install** untuk memulai proses instalasinya.

Gambar 4.10 Folder instalasi

6. Tunggu proses instalasi dilakukan sampai selesai.

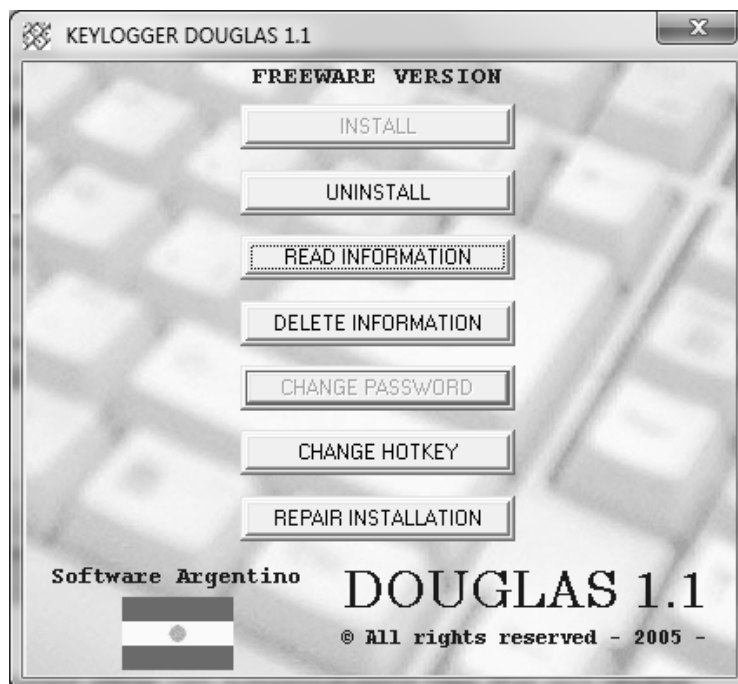
Gambar 4.11 Proses instalasi sedang dilakukan

7. Kini proses instalasi telah sukses dilakukan, klik saja **OK**.

Gambar 4.12 Proses instalasi selesai

Sekadar informasi tambahan saja, apabila Anda tidak bisa melakukan instalasi Douglas tersebut, coba matikan Antivirus Anda terlebih dahulu. Karena pada beberapa kasus, Douglas juga dianggap sebagai virus. Selain itu, kasus yang sering terjadi adalah file instalasi hilang sewaktu Anda mengekstrak dari file kompresinya.

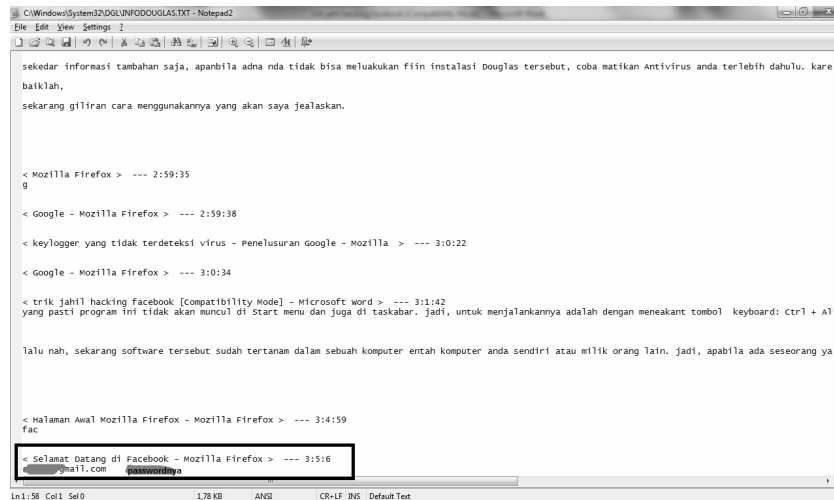
Gambar 4.13 Terdeteksi sebagai program berbahaya

Baiklah, sekarang giliran cara menggunakannya yang akan saya jelaskan.

Yang pasti, program ini tidak akan muncul di Start menu dan juga di taskbar. Jadi, untuk menjalankannya adalah dengan menekan tombol keyboard: **Ctrl** + **Alt** + **Shift** + **F9**.

Gambar 4.14 Keylogger Douglas berjalan

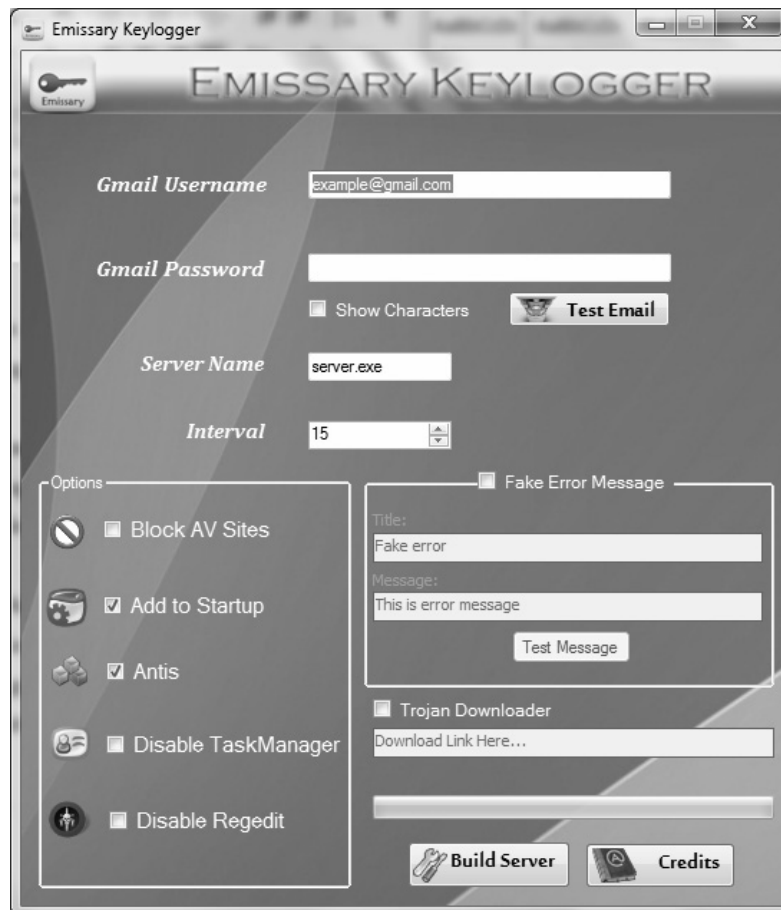
Nah, sekarang software tersebut sudah tertanam dalam sebuah komputer, entah komputer Anda sendiri atau milik orang lain. Jadi, apabila ada seseorang yang membuka facebook lalu memasukkan username dan password-nya maka akan dicatat otomatis oleh program tersebut.

Untuk melihat informasi yang direkam, jalankan program Douglas lalu klik tombol **Read Information**.

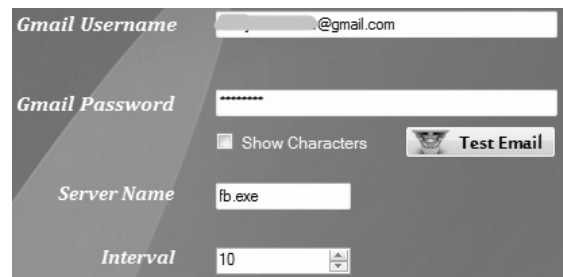
Berikut ini hasil rekaman Douglas yang telah berhasil mencuri password facebook seseorang.

Gambar 4.15 Hasil rekaman Keylogger Douglas

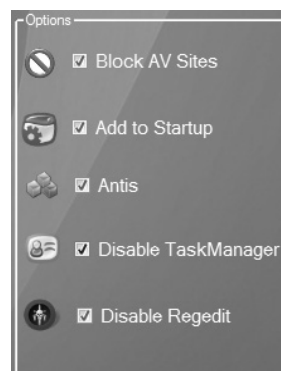
Selain informasi password, Anda bisa melihat apa pun yang saya ketik akan direkam oleh keylogger tersebut.

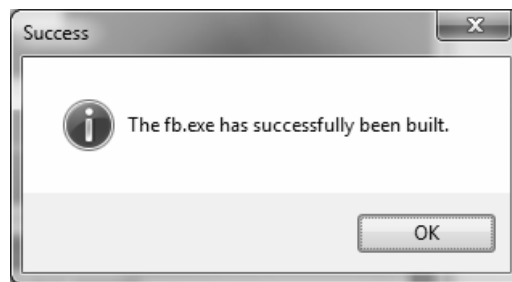
Sekarang saya akan menjelaskan sebuah program keylogger lain-nya, yang bernama Emissary Keylogger, Anda bisa mendapat-kannya di internet. Sekali lagi, saya ingatkan jangan lupa men-disable Antivirus terlebih dahulu.

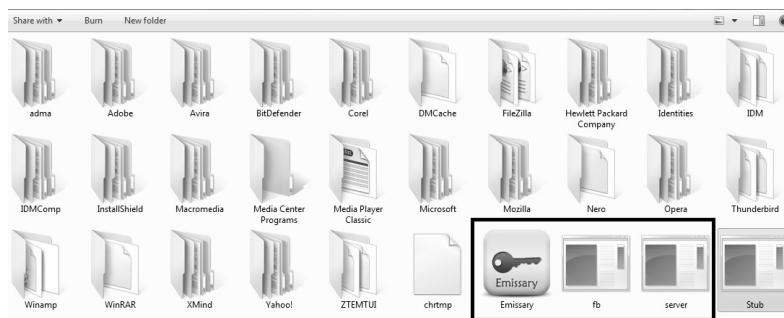
Berikut tampilan program Emissary Keylogger.

Gambar 4.16 Emissary Keylogger

Cara menggunakannya adalah:

1. *Gmail Username*: Isi dengan account Gmail.
2. *Gmail Password*: masukkan password Anda.
3. *Server Name*: isi dengan nama yang Anda suka, sebagai nama keylogger-nya, seperti fb.exe.
4. *Interval* menunjukkan hasil log yg akan dikirim ke email Anda setiap 15 menit atau Anda bisa mengganti sendiri waktunya.

Gambar 4.17 Menjalankan Emissary Keylogger

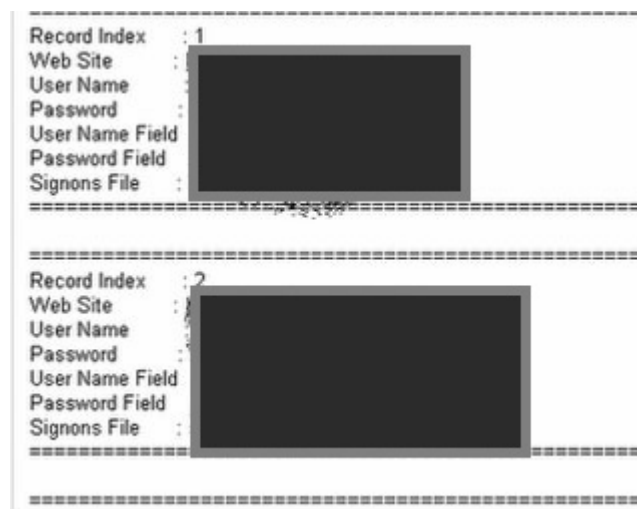
5. Pada bagian *Options*: kasih tanda centang pada semua pilihan sehingga tidak terdeteksi oleh Task Manager & Regedit.
   - Blok AV Sites: VirusScanning Blok Situs-situs Web pada komputer korban
   - Add to Startup: Menambahkan untuk Startup melalui Registry
   - Antis: Anubis, BitDefender, Kaspersky, KeyScrambler, Malwarebytes, NOD32, Norman, OllyDbg, Outpost, Wireshark
   - Disable TaskManager: TaskManager Nonaktifkan pada PC korban
   - Nonaktifkan Regedit: Nonaktifkan Regedit pada PC korban

Gambar 4.18 Mengatur opsi

6. Berikan tanda centang pada “Trojan Downloader”.
7. Sekarang klik tombol **Build Server**.
8. Maka akan muncul pesan yang menyatakan bahwa pembuatan file server telah selesai dibuat, klik saja tombol **OK**.

Gambar 4.19 File server telah dibuat

9. Sekarang Anda memiliki file fb.exe atau sesuai dengan nama yang Anda masukkan sebagai server. File tersebut akan dibuat dalam folder aplikasi Anda. Atau bisa juga dibuat pada lokasi lain, seperti C:\Users\Nama-User-Anda\AppData\Roaming. Apabila tidak ada, Anda bisa melakukan *searching*.

Gambar 4.20 Melihat File server yang telah dibuat

10. Untuk melakukan pencarian account facebook dan password, Anda harus mengirim file ini ke server korban dan membuatnya menginstalnya pada komputer. Anda dapat menggunakan Binder, crypter, atau Fake Hacking Software

untuk mengikat server file ini. Atau, Anda juga bisa mengombinasikannya dengan file MP3. Atau Anda pura-pura saja pinjam komputer korban dan jalankan sendiri. Sehingga setiap kali korban menjalankan file mp3, server secara otomatis terinstal di komputer tanpa sepengetahuannya. Untuk melakukan pengikatan atau penggabungan tersebut tidak akan saya bahas karena di luar jalur buku ini. Mungkin Anda bisa membaca beberapa buku Hacking, seperti "Buku Sakti Hacker", "Instant Hacking", atau buku "Worm Undercover".

11. Selanjutnya, apabilah korban menjalankan file keylogger yang Anda pasang atau Anda kirim maka dia akan bekerja mencari password dan mengirimkan email yang berisi semua user-id dan password ke email Anda.

Gambar 4.21 Menemukan password facebook

Jika Anda perhatikan, ada banyak keylogger yang bisa digunakan sebenarnya. Dan kebanyakan dari keylogger tersebut akan terdeteksi sebagai virus oleh antivirus. Oleh karena itu, Anda bisa menggunakan beberapa keylogger berikut ini yang tidak terdeteksi sebagai virus. Setidaknya sewaktu penulisan teks ini dilakukan, masih tidak terdeteksi sebagai virus.

1. Revealer keylogger.

   Anda bisa memperolehnya di: http://www.logixoft.com/

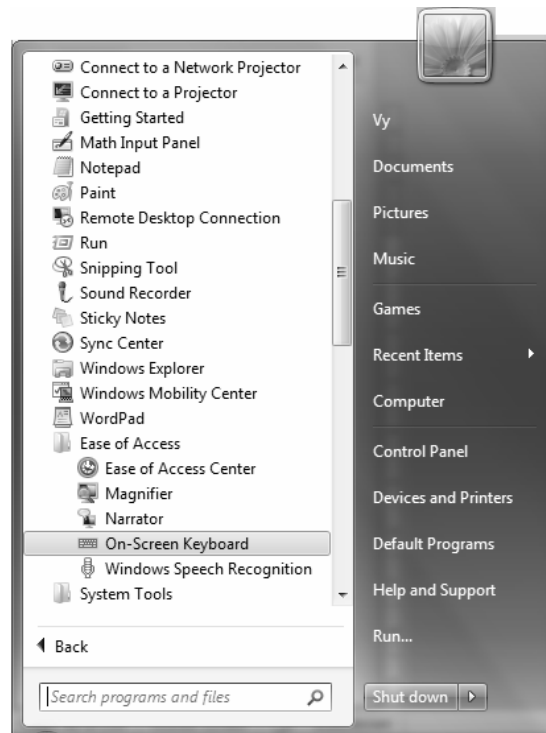
Gambar 4.22 Revealer keylogger

2. REFOG Free Keylogger
3. Quick FREE Keylogger
4. Actual Keylogger
5. 007 Keylogger

Mengatasi Keylogger

Untuk mengatasi kasus keylogger ini, Anda disarankan untuk tidak memasukkan password secara langsung melalui keyboard. Sebagai solusinya, Anda bisa memanfaatkan Virtual Keyboard yang telah disediakan oleh Windows.

Untuk menjalankan Virtual Keyboard, lakukan langkah berikut:

1. Klik **Start** → **All Programs** → **Accessories** → **Ease of Access**, dan klik **On Screen Keyboard**.

Gambar 4.23 Menjalankan Onscreen Keyboard

2. Berikut ini tampilan Virtual keyboard yang terdapat pada Windows 7.

Gambar 4.24 Virtual Keyboard atau On-screen keyboard

Cara penggunaannya cukup mudah, Anda hanya perlu meletakkan posisi kursor pada bagian untuk mengisi password. Lalu tekan huruf yang menjadi password Anda yang muncul pada virtual keyboard tersebut, atau dikenal juga dengan nama On-Screen Keyboard.